## REMARKS

The last Office Action of March 31, 2009 has been carefully considered. Reconsideration of the instant application in view of the foregoing amendments and the following remarks is respectfully requested.

Claims 1-22 are pending in the application. Claims 1, 11 have been amended by inoporating the subject matter of claims 13 and 16, respectively. Claims 23, 24 have been added to recite features deleted from claims 1 and 11, respectively. Claims 13, 16 have been canceled. No amendment to the specification has been made. No fee is due.

## CLAIM REJECTIONS - 35 U.S.C. §112, SECOND PARAGRAPH

Claims 1, 11 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The rejection under 35 U.S.C. 112, second paragraph, is hereby respectfully traversed.

Applicant's invention is directed to solving the problem described in paragraphs **[0003]** to **[0008]** of the present application. In particular, fewer repair technicians are needed if an industrial plant is highly automated. Technicians do not need to be on site at all times in such plants. However, to be able to prevent machine failures from causing costly damage and loss of productivity, the roving technicians who remotely supervise highly-automated industrial plants need immediate, real-time access to all the detailed information in the database of each controller that is operating the automated machines in those plants. The competitive and financial-market implications of information about the product throughput and production downtime make it sensitive, business confidential information, as is well known.

Furthermore, when a plant is remotely operated, allowing unauthorized persons to access any of the machine controllers that are installed in that plant, or to access the detailed machine information used by the technicians, can expose the company to legal liability and possibly also to sabotage, as is well known. Thus, it is well-known that such information is "sensitive" in that it must be PKI encrypted. The more detailed information that is available to be accessed, the more important it is to protect the information that is being accessed from unauthorized access. **[0006]**

Conventional machine controllers are capable of sending e-mail alert messages to technicians when alarm events occur and use PKI encryption to protect the sensitive industrial information contained in those alert messages. **[0006]** However, PKI encryption is not suitable to provide this sensitive industrial information to the roving technicians who are often not "at their company's location". **[0007]** Thus, PKI-encrypted e-mails cannot be used to provide that "sensitive" event-relevant information to roving technicians. "A cryptographically protected communication protocol based on an Internet browser" is used, instead, to obtain information from the controller of the particular machine where the alarm event occurred. **[0024] - [0025]** The draw back to PKI encryption of this sensitive information is that it is logistically complex, and too inflexible for use by roving technicians.

The "sensitive" information is the information referred to in paragraph **[0024]** information that, for the sake of security, would have to be sent in the conventional PKI-encrypted e-mails to the non-roving technicians "at their company's location". **[0007]** This "sensitive" information that must be PKI encrypted is well-known in the art, as explained in applicant's disclosure. **[0006] - [0007]**

Thus the nature of the "sensitive" information recited in the claims is well-known in the art that PKI encrypts the machine data contained in alert message e-mails sent to these technicians, and is not indefinite. Withdrawal of the rejection of the claims 1 and 11 under 35 U.S.C. §112, second paragraph is thus respectfully requested.

Withdrawal of the rejection under 35 U.S.C. §112, second paragraph is thus respectfully requested.

## CLAIM REJECTIONS - 35 U.S.C. §102

Claims 1-4, and 7-22 stand rejected under 35 U.S.C. §102(e) as being anticipated by published U.S. Pat. Appln. No. 2008/0186166 of Zhou et al.

The rejection under 35 U.S.C. 102(e) is respectfully traversed in view of the amendments to independent claims 1 and 11 and the following remarks.

Claims 1 and 11 have been amended to recite that "event-relevant information" is written to the database, as recited in the preamble, and that the database to which that event-relevant information is written is a database in the controller, as shown in Fig. 1. The step of "performing at least one of failure analysis or fault repair on the machine using the sensitive event-relevant information accessed using said cryptographically protected communication protocol" has also been added to claims 1 and 11, as recited in cancelled claims 13 and 16.

In accordance with applicant's disclosed invention, when an alarm event occurs in one of the many industrial controllers installed in a company's remotely-operated industrial plants, the sensitive machine information that would conventionally be sent by the industrial controller to the company's offices using PKI encryption is remains in the controller's database, instead. This is highly advantageous because the technician who is qualified to respond to the particular type of alarm event that has occurred often must provide failure analysis and fault repair to machines located at multiple plant locations. Therefore, this technician is often not reachable at the office.

To provide the timely failure analysis and fault repair needed to minimize machine downtime and preserve a plant's profitability, the controller that detects an alarm event in a machine it controls must remotely provide this roving technician the same real-time access to the data in the controller's database that this technician would have when working directly on that controller at the controller's location in the plant, not just some selectively reported parameters that are periodically stored by some Website.

Thus, in accordance with applicant's claimed invention, this sensitive information remains in the database of the industrial controller that has been controlling the affected machine when a receiver-specific alert message is sent to a specified remote receiver. Thus, the complete set of sensitive industrial machine data being used by the industrial controller, data that a technician would have access to when working directly on the controller at the controller's location, will also be immediately remotely available to a roving technician. Furthermore, additional information will be immediately available to that technician in real-time after the alarm event has occurred in the machine, as further information that is generated by the affected machine is received by its controller's own database.

In accordance with applicant's claimed invention, the information in the database of that industrial controller is accessed by the technician to whom the alert was sent through a Web server using a cryptographically protected communication protocol based on an Internet browser. However, to obtain the most complete and up-to-date failure analysis and fault repair information, the controller's database is directly accessed by that technician, not just the web server's database.

In contrast, Zhou in paragraph **[0111]** describes a Website provided by the web server of an ASP (200). The Website provides these end users (25) remote access to GPS data and selected monitoring data from portable monitoring devices (100) attached to a patient, child, or shipment, respectively, that is stored and analyzed by the Website.

Zhou's Website enables end users (25), such as healthcare providers, parents, or businesses, to update the configuration of the portable monitoring devices (100). Updating the configuration of these portable monitoring devices (100) allows the users (25) to select or change: 1) the patient, child, or shipment parameters that are reported to the Website by the portable monitoring devices (100), and 2) the frequency of data collection by the Website from the portable monitoring devices (100). **[0111]**

When a user receives an electronic alert message from the ASP (200) or from the ASP's live CMC operators (40), a computer, PDA, or WAP-enabled cell phone is used by the user (25) to access the data that is supplied by the portable monitoring devices (100) to the ASP's Website. **[0021]** - **[0022]** Paragraph **[0022]** discloses using a PIN to access the patient, child, or shipment information stored on Zhou's Website though the CMC operators (40). Paragraph **[0023]** discloses using SSL encryption to access that information on Zhou's Website.

Nothing in Zhou discloses or suggests using a modem connection protected by an authentication protocol, as recited in claim 11, for accessing the patient, child, or shipment parameters that the monitoring devices (100) provide to Zhou's Website.

Nothing in Zhou discloses or suggests accessing event-relevant data in a controller's database, as recited in claims 1 and 11, rather than accessing the data on a Website. Instead of providing access to all the event-relevant data in a controller's database, Zhou has the user select which data Zhou's Website will receive and, also, how often Zhou's Website will store that data. **[0111]**

Nothing in Zhou discloses or suggests accessing data from "a controller", rather than from a monitoring device.

Nothing in Zhou discloses or suggests accessing data directly from a "database in the controller", rather than a copy of that data that is stored on Zhou's Website.

Furthermore, as noted above, the data that is accessed from Zhou's Website using SSL or a PIN is too fragmentary and too stale for use in failure analysis and fault repair. Successful failure analysis and fault repair both require the access to event-relevant data in the controller's database that an on-premises technician would have. The data accessed on Zhou's Website only includes selected monitored parameters, not the event-relevant control parameters that controllers receive in real time from the machines they control. Thus, nothing in Zhou discloses or suggests using the data that is accessed by a user on Zhou's Website for the failure analysis and fault repair recited in claims 1 and 11. The information on Zhou's website is not suitable for that use. Successful failure analysis and fault repair require real-time access to the controller's own fault-relevant control parameter information.

For the reasons set forth above, it is applicant's contention that Zhou neither teaches nor suggests the features of the present invention, as recited in independent claims 1 and 11.

Claims 2-4, 7-10, 12-14, 21, 23 which depend from claim 1 and therefore contain all the limitations thereof, and claims 15-20, 22, 24 which depend from claim 11 and therefore contain all the limitations thereof, patentably distinguish over the applied prior art in the same manner as claims 1 and 11, respectively.

Withdrawal of the rejection under 35 U.S.C. §102(e) is thus respectfully requested.

## CLAIM REJECTIONS - 35 U.S.C. §103

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Zhou et al. in view of Qi et al. (US 6892064).

Claim 6 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Zhou et al. in view of published U.S. Pat. Appln. No 2007/0208697 of Subramaniam et al.

Claims 5, 6, which contain all the limitations of claim 1, patentably distinguish over the applied prior art in the same manner as claim 1.

Withdrawal of the rejection under 35 U.S.C. §103(a) is thus respectfully requested.

## CONCLUSION

In view of the above presented remarks and amendments, it is respectfully submitted that all claims on file should be considered patentably differentiated over the art and should be allowed.

Reconsideration and allowance of the present application are respectfully requested.

Should the Examiner consider necessary or desirable any formal changes anywhere in the specification, claims and/or drawing, then it is respectfully requested that such changes be made by Examiner's Amendment, if the Examiner feels this would facilitate passage of the case to issuance. If the Examiner feels that it might be helpful in advancing this case by calling the undersigned, applicant would greatly appreciate such a telephone interview.

Respectfully submitted,

By:____________________
Henry M. Feiereisen
Agent For Applicant
Reg. No: 31,084

Date: June 30, 2009
708 Third Avenue
Suite 1501
New York, N.Y. 10017
(212)244-5500
HMF/RL:af